AMENDMENTS TO THE CLAIMS

1.   (Currently Amended) An authenticating device comprising:

an authentication processing unit to perform an authentication process with an authenticated device using an authentication key; and

an update key generating unit to generate a new authentication key when the authenticated device does not hold an the authentication key to be used in the authentication process by the authentication processing unit, and to generate a the new authentication key for updating an the authentication key to be used in the authentication process by the authentication processing unit when the authenticated device holds the authentication key but the authentication process with the authenticated device by the authentication processing unit fails,

wherein the authentication processing unit performs the authentication process with the authenticated device again based on a prescribed algorithm identifier and a prescribed encryption key identifier, using the new authentication key generated by the update key generating unit.

2.   (Currently Amended) The authenticating device of claim 1, further comprising a receiving unit to receive a the prescribed algorithm identifier and a the prescribed encryption key identifier from the authenticated device,

wherein the update key generating unit generates the new authentication key based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the receiving unit,

the authenticating device, further comprising a transmitting unit to transmit the new authentication key generated by the update key generating unit to the authenticated device,

wherein the authentication processing unit performs the authentication process with the authenticated device again, using the new authentication key transmitted by the transmitting unit.

DRA/AMI/bms

Application No. 10/584,193   Docket No.: 2565-0296PUS1
Amendment dated October 14, 2009
Reply to Notice of Non-Compliant of October 13 , 2009

3.   (Previously Presented) An authenticated device comprising:

a memory unit to store a prescribed algorithm identifier and a prescribed encryption key identifier;

an authentication processing unit to perform an authentication process with an authenticating device using an authentication key;

a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier stored by the memory unit, to the authenticating device when the authenticated device holds the authentication key but the authentication process with the authenticating device by the authentication processing unit fails; and

a receiving unit to receive from the authenticating device a new authentication key based on the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the transmitting unit,

wherein the authentication processing unit performs the authentication process with the authenticating device again, using the new authentication key received by the receiving unit.

4.   (Original) The authenticated device of claim 3,

wherein the receiving unit receives prescribed information from the authenticating device when the authentication process with the authenticating device by the authentication processing unit fails, and

wherein the transmitting unit transmits the prescribed algorithm identifier and the prescribed encryption key identifier stored by the memory unit, when the prescribed information has been received by the receiving unit.

                     DRA/AMI/bms

5.   (Cancelled)

6.   (Original) A key updating method comprising:

transmitting prescribed information from an authenticating device to an authenticated device when an authentication process fails, the authentication process being performed between the authenticated device which stores a prescribed algorithm identifier and a prescribed encryption key identifier, and the authenticating device, using an authentication key;

receiving the prescribed information transmitted from the authenticating device, at the authenticated device;

transmitting from the authenticated device to the authenticating device, the prescribed algorithm identifier and the prescribed encryption key identifier stored, after the prescribed information is received;

receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted at the authenticating device;

generating a new authentication key, based on the prescribed algorithm identifier and the prescribed encryption key identifier received, at the authenticating device;

transmitting the new authentication key generated to the authenticated device;

receiving the new authentication key transmitted at the authenticated device;'

executing a key update using the new authentication key received, as an update key to perform the authentication process between the authenticated device and the authenticating device;

generating and transmitting an update confirmation data to the authenticating device; and

receiving and checking the update confirmation data.

DRA/AMI/bms

7.   (Previously Presented) A computer readable storage medium having stored thereon computer executable program for performing an authentication process, the computer program when executed causes a processor to execute steps of:

transmitting prescribed information from an authenticating device to an authenticated device when an authentication process fails, the authentication process being performed between the authenticated device which stores a prescribed algorithm identifier and a prescribed encryption key identifier, and the authenticating device, using an authentication key;

receiving the prescribed information transmitted from the authenticating device, at the authenticated device;

transmitting from the authenticated device to the authenticating device, the prescribed algorithm identifier and the prescribed encryption key identifier stored, after the prescribed information is received;

receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted at the authenticating device;

generating a new authentication key, based on the prescribed algorithm identifier and the prescribed encryption key identifier received, at the authenticating device;

transmitting the new authentication key generated to the authenticated device;

receiving the new authentication key transmitted at the authenticated device;

executing a key update using the new authentication key received, as an update key to perform the authentication process between the authenticated device and the authenticating device;

generating and transmitting an update confirmation data to the authenticating device; and

receiving and checking the update confirmation data.

DRA/AMI/bms